A good way to start an information security threat assessment is to include everyone who might be affected by an information security breech in an information security threat Brainstorm. Brainstorming is a highly effective 'crowd sourcing' technique, that will help you identify your critical threats. But more than that, Brainstorming is an exercise in inclusivity, involvement, taking everyones views seriously and in educating and raising awareness.

The following generic list of potential threats is by no means complete, I can say that with certainty and, anyway, new threats arrive all of the time, but it represents a good starting point for such a Brainstorm.

Nature and Accidents

1. Earthquakes
2. Landslides
3. Volcanoes
4. Fires
5. Storms and floods
6. Transportation accidents (car, aviation etc..)
7. Hazardous materials related events
8. Solar flares

Current and Past Employees

1. Human error
2. Sabotage
3. Tampering
4. Vandalism
5. Theft
6. Unions, strikes and labour actions
7. Pandemics and disease
8. Insider trading
9. Fraud
10. Liability for employee actions
11. Scandals
12. Corporate crime
13. Discriminatory abuse
14. Workplace bullying
15. Sexual harassment
16. Professional misconduct
17. Negligence
18. Passive–aggressive behaviour
19. Workplace revenge

20. Insurance fraud
21. Lawsuits against employer

Competitors
1. Industrial espionage
2. Intellectual property theft
3. Copyright infringement
4. Mudslinging
5. Illegal infiltration
6. Dirty tricks
7. Patent infringement
8. Competitive research
9. Price surveillance

The Press
1. Bad publicity
2. Exposing trade secrets
3. Exposing strategy and new products

Litigants
1. Seeking confidential data as evidence

Hackers
1. IP Spoofing
2. Social engineering
3. Man-in-the-middle spoofing
4. DNS Poisoning
5. Trojan
6. Cracks
7. Worms
8. Viruses
9. Eavesdropping
10. Spam
11. Phishing
12. Spyware
13. Malware
14. Password Cracking
15. Network sniffing
16. Back door/trap door
17. Tunnelling
18. Website defacement

19. TCP/IP hijacking
20. Replay Attacks
21. System tampering
22. System penetration

Criminals

1. Kidnapping
2. Bribery
3. Extortion
4. Fraud
5. Theft
6. Physical infrastructure attacks
7. Information blackmail
8. Assault
9. Sale of stolen information
10. Cyberstalking

Governments, Terrorists and Political Organisations

1. Acts of war (conventional)
2. Nuclear war
3. Biological warfare
4. Chemical warfare
5. Computer warfare (including physical disruption of communication satellites etc..)
6. Espionage
7. Terrorism
8. Cyberwarfare
9. Electromagnetic weapons
10. Wiretapping